TCP Attacks Lab

NT140.O11.ANTT

Thành viên:

Nguyễn Đình Luân – 21521105

Trần Thanh Triều - 21522713

Trần Đức Trí Dũng - 21520748

Task 1.1

Code:

A computer screen with white text

Description automatically generated

Chạy chương trình trên máy attacker:

A black background with white text

Description automatically generated

Xem các kết nối trên victim

A screenshot of a computer screen

Description automatically generated

Trên máy user1 ta tiến hành telnet:

A computer screen with white text

Description automatically generated

Như đã thấy ta vẫn có thể kết nối  
Thử giảm queue size còn 80 và flush tcp\_metrics

A screen shot of a computer

Description automatically generated

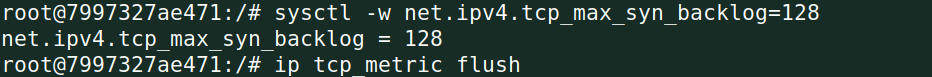
Tiến hành tấn công lại và ta đã thành công, không thể telnet đến máy victim:

A black background with white text

Description automatically generated

Task 1.2

Ta đặt lại queue về giá trị mặc định là 128 sau đó tiến hành chạy file attack



A green background with white text

Description automatically generated

A screenshot of a computer screen

Description automatically generated

Ta thấy rằng tấn công thành công mà không cần giảm queue, không giống như task 1.1

A green screen with white text

Description automatically generated

Task 1.3:

Bật syn cookie



Kết quả khi chạy code C:

A screenshot of a computer

Description automatically generated

Kết quả khi chạy python:

A screenshot of a computer screen

Description automatically generated

Cả 2 trường hợp ta đều có thể telnet, vậy tính năng syn cookie đã hoạt động tốt

Task 2:

Telnet bằng máy user1 đén victim sau đó capture kết nối telnet bằng wireshark, ta có các thông tin cần thiết để điền vào chương trình:



Code:

A computer screen with a number of text

Description automatically generated with medium confidence

Ta chạy code:

A screenshot of a computer program

Description automatically generated

Kết nối telnet bị ngắt

A computer screen shot of a computer

Description automatically generated

Kiểm tra bằng netstat trên victim:

A computer screen with white text

Description automatically generated

Task 3:

Code: chương trình này sẽ tự động ghi đè vào file có tên hịjacking.out khi bắt được kết nối tcp đến máy victim đồng thời in ra thông tin gói tin trên máy attacker

A screen shot of a computer code

Description automatically generated

Telnet từ máy user1:

A computer screen shot of a computer

Description automatically generated

Chạy file tấn công:

A computer screen shot of a program

Description automatically generated

Kiểm tra kết quả:

A black background with white text

Description automatically generated

Task4:

Code:ta sửa code bên trên 1 chút để có thể mở shell

A screen shot of a computer code

Description automatically generated

Ta mở port 9090 tên máy attacker sau đó telnet đến máy victim bằng máy user1:

telnet:

A screenshot of a computer

Description automatically generated

Chạy chương trình:

A green screen with white text

Description automatically generated

Đã mở được Shell:

A screenshot of a computer

Description automatically generated